SOC Concepts and Questions

Contents

IOC and IOA

Indicators of Compromise (IOC) and Indicators of Attack (IOA) are critical concepts used to detect, understand, and respond to security incidents.

Indicators of Compromise (IOC)

- **Definition**: IOCs are pieces of **forensic data that suggest a potential breach or malicious activity**. They are artifacts observed on a network or in operating systems that indicate a security incident may have occurred.
- **Examples**:
  - **Unusual network traffic**
  - **Malicious code signatures**
  - **IP addresses, URLs, or domain names associated with known threats**
- **Usage**: **IOCs help in detecting past and ongoing intrusions**. They are typically used in reactive security measures, such as after a breach has been detected.

Indicators of Attack (IOA)

- **Definition**: IOAs focus on **detecting the intent and methods used by attackers to achieve their objectives.** Unlike IOCs, which are often specific and static, **IOAs are more about understanding the behavior and tactics of the attacker.**
- **Examples**:
  - **Patterns of behavior** that indicate an attacker is attempting to compromise a system
  - **Unusual activity** that aligns with known attack techniques (e.g., lateral movement within a network)
  - **Sequence of actions** that deviate from normal usage patterns
  - **Use of legitimate tools in unusual ways** (e.g., PowerShell used to download malware)
- **Usage: IOAs are used to identify and prevent potential attacks before they cause damage.** They are proactive and help in understanding and mitigating the attacker's strategy and techniques.

Comparison

- **Focus**:
  IOCs are evidence of an incident
  IOAs are indicators of potential malicious activity based on behavior.
- **Timeframe**:
  IOCs are often used in post-incident analysis
  IOAs are used for real-time or near-real-time detection and prevention.
- **Nature**:
  IOCs are often static and specific
  IOAs are dynamic and behavior-based

Threat Intelligence

Threat intelligence is the practice of gathering, analyzing, and utilizing information about potential or current threats to an organization's security.
It provides context and actionable insights that help organizations understand, anticipate, and defend against cyber threats.

Key Aspects of Threat Intelligence

1. **Data Collection**:
    - **Sources**: Threat intelligence data can be collected from various sources, including open-source intelligence, dark web monitoring, internal logs, network traffic, social media, and commercial threat intelligence feeds.
    - **Types of Data**: This includes IOCs, IP addresses, URLs, domain names, malware hashes, and details about threat actors and their tactics, techniques, and procedures (TTPs).
2. **Analysis**:
    - **Correlation and Context**: Analyzing the collected data to find correlations, patterns, and context.
    - **TTPs**: Understanding the tactics, techniques, and procedures of threat actors to predict and mitigate future attacks.
3. **Utilization**:
    - **Proactive Defense**: Using threat intelligence to anticipate and prevent potential threats by strengthening defenses and improving security posture.
    - **Incident Response**: Leveraging threat intelligence during and after an incident to understand the nature of the attack, identify the attackers, and take appropriate remediation steps.

Benefits of Threat Intelligence

- **Faster Response**.
- **Risk Mitigation**
- **Enhanced Detection and Prevention**.
- **Informed Decision-Making.**

Conclusion

Threat intelligence is a critical component of modern cybersecurity strategies. By gathering, analyzing, and utilizing information about potential threats, organizations can better defend against cyber-attacks, respond more effectively to incidents, and make informed decisions to enhance their overall security posture.

Some well-known Threat Intelligence:

1. **IBM X-Force Exchange.**
2. **Cisco Talos Intelligence.**
3. **AbuseIPDB.**
4. **Virustotal.**

System Hardening

System hardening is the process of securing a computer system by reducing its surface of vulnerability.

This involves configuring the system to minimize potential attack vectors, removing unnecessary services and software, and applying security measures to protect against threats.

Steps in System Hardening

1. **Remove Unnecessary Services and Software**:
   - **Disable Unneeded Services**.
   - **Uninstall Unnecessary Software**.
2. **Apply Security Patches and Updates**:
   - **Regular Updates**.
   - **Automated Updates**.
3. **User Accounts and Authentication**:
   - **Strong Password Policies.**
   - **Limit Administrative Privileges**.
   - **Multi-Factor Authentication (MFA).**
4. **Network Security Measures**:
   - **Firewalls**: Configure firewalls to control incoming and outgoing traffic based on predefined security rules.
   - **Intrusion Detection and Prevention Systems (IDPS)**: Deploy IDPS to monitor network traffic for suspicious activity.
5. **Implement Logging and Monitoring**:
   - **System Logs**.
   - **Monitoring Tools**.
6. **Data Protection**:
   - **Encryption**.
   - **Backup**.

Benefits of System Hardening

- **Reduced Attack Surface**: By minimizing the number of potential entry points, system hardening makes it more difficult for attackers to exploit vulnerabilities.
- **Performance**: Removing unnecessary services and software can improve system performance and stability.
- **Improved Security Posture**.

Conclusion

System hardening is a vital practice in cybersecurity aimed at reducing the risk of compromise by securing systems against potential threats. By following best practices for system hardening, organizations can protect their critical assets, maintain compliance, and improve their overall security posture.

Privilege escalation

This is often a crucial step in many cyber-attacks, allowing the attacker to move from a lower-privileged account (such as a standard user) to a higher-privileged account (such as an administrator or root).

Types of Privilege Escalation

1. **Vertical Privilege Escalation**: Occurs when an attacker gains higher-level privileges than initially granted. For example, a normal user account gaining administrative rights.
2. **Horizontal Privilege Escalation**: Occurs when an attacker accesses resources or functionalities of other users with similar privileges. For example, accessing another user's data or account.

Common Methods of Privilege Escalation

1. **Exploiting Software Vulnerabilities**:
   - **Buffer Overflow**: Overflowing a buffer to overwrite adjacent memory and execute malicious code with higher privileges.
   - **Zero-day Exploits**: Using unknown vulnerabilities to gain elevated access.
2. **Misconfigurations**:
   - **Insecure Permissions**: Exploiting weak file or directory permissions to gain access to sensitive data or executables.
3. **Credential Theft**:
   - **Keylogging**: Recording keystrokes to capture administrative credentials.
   - **Pass-the-Hash**: Using hashed password values to authenticate without knowing the actual password.
4. **Social Engineering**:
   - **Phishing**: Trick users into revealing their credentials or executing malicious payloads that grant elevated access.
5. **Malicious Software**:
   - **Trojan Horses** and **Rootkits**

Preventive Measures

1. **Patch Management**.
2. **Principle of Least Privilege**:
3. **Strong Authentication**: **Multi-Factor Authentication** and **Secure Credential Storage**:

Conclusion:

Privilege escalation is a significant threat in cybersecurity, enabling attackers to gain unauthorized access to sensitive systems and data. By understanding the methods used and implementing robust security measures, organizations can mitigate the risks associated with privilege escalation attacks.

Persistence

Persistence refers to the techniques used by attackers to maintain their foothold on a compromised system, even after restarts, user logouts, or other attempts to disrupt their access.

Some Methods of Persistence

1. **AutoStart Entries:**
   - **Registry Keys (Windows)**: Modifying Windows registry keys to launch malicious programs at startup.
   - **Startup Folders (Windows)**: Placing malicious shortcuts in startup folders to execute on system boot.
2. **Scheduled Tasks**:
   - **Task Scheduler (Windows)**: Creating or modifying scheduled tasks to execute malicious payloads at specific times or intervals.
3. **Rootkits**:
   - **Rootkits**: Installing rootkits to hide the presence of malicious software and provide ongoing access.
4. **User and System Accounts**:
   - **Backdoor Accounts**: Creating hidden user accounts with administrative privileges for remote access.
   - **Credential Theft**: Stealing and using legitimate credentials to maintain access.
5. **DLL Injection and Hijacking**:
   - **DLL Injection**: Injecting malicious code into legitimate processes.
   - **DLL Hijacking**: Replacing legitimate dynamic link libraries (DLLs) with malicious ones.
6. **Network-based Persistence**:
   - **Remote Access Trojans (RATs)**: Using RATs to maintain remote control over compromised systems.
   - **Command and Control (C2) Channels**: Establishing covert communication channels to issue commands and exfiltrate data.

Conclusion

Persistence is a critical component of advanced cyber-attacks, enabling attackers to maintain control and achieve their objectives over time. Understanding and detecting persistence mechanisms is essential for effective incident response and system hardening efforts.

Lateral movement

Techniques used by attackers to move within a network after initially compromising a system. This movement allows attackers to navigate through the network to gain access to additional systems and data.

Lateral movement is a critical phase in many advanced persistent threats (APTs) and can be difficult to detect because it often involves using legitimate credentials and tools.

Techniques for Lateral Movement

1. **Credential Dumping**:
   - **Definition**: Extracting credentials (user and pass) from compromised systems.
   - **Tools**: Attackers use tools like Mimikatz, Windows Credential Editor (WCE), …
2. **Pass-the-Hash**: Using hashed credentials to authenticate without needing to decrypt them.
3. **Pass-the-Ticket:**
   - **Definition**: Using Kerberos tickets to authenticate.
   - **Method**: Attackers steal Kerberos tickets (TGTs or TGSs) from memory and use them to access other systems in the network.
4. **Remote Execution**:
   - **Tools**: Attackers use tools like PsExec, Windows Management Instrumentation (WMI), Remote Desktop Protocol (RDP), and Secure Shell (SSH) to execute commands on remote systems.
5. **Service Creation**: Creating or modifying services on remote systems to maintain persistence or execute malicious code.

Detecting and Preventing Lateral Movement

1. **Network Segmentation**: Dividing into smaller segments to limit the spread of attacks.
2. **Least Privilege Principle**.
3. **Monitoring and Logging**: Tracking activities across the network to detect suspicious behavior.
4. **Multi-Factor Authentication (MFA)**.
5. **Behavioral Analysis**.
6. **Endpoint Detection and Response (EDR)**.
7. **Patch Management**.
8. **Regular Audits and Penetration Testing**.

Conclusion:

Lateral movement is a sophisticated and stealthy phase of cyber-attacks, enabling attackers to expand their control and access within a network. Understanding the techniques used for lateral movement and implementing robust detection and prevention measures are critical for enhancing network security and protecting against advanced threats.

SANS Incident Response Steps

1. Preparation:

- **Establish Policies and Procedures**: Define incident response policies, procedures, and guidelines tailored to the organization's needs.
- **Form Incident Response Team**: Identify and assemble a team of individuals with specific roles and responsibilities for incident response.
- **Tools and Resources**: Ensure availability and readiness of necessary tools, resources, and technologies for incident detection, analysis, and response.
- **Training and Awareness**: Conduct regular training sessions and awareness programs for incident response team members and relevant stakeholders.

2.Identification:

- **Incident Notification**: Detect and receive alerts or reports of potential security incidents from various sources, such as monitoring systems, users, or automated detection tools.
- **Initial Triage**: Conduct initial triage to determine the nature and scope of the incident, prioritize response actions, and gather preliminary information.

3.Containment:

- **Contain the Incident**: Implement containment measures to prevent further damage or spread of the incident while maintaining essential business operations.
- **Isolation**: Isolate affected systems or networks to minimize impact and prevent the compromise from spreading to other parts of the infrastructure.

4.Eradication:

- **Root Cause Analysis**: Identify the root cause of the incident and determine the specific vulnerabilities or weaknesses exploited by the attacker.
- **Remediation**: Develop and implement corrective actions, patches, or configurations to eliminate the root cause and prevent similar incidents in the future.

5.Recovery:

- **Data Restoration**: Restore affected systems, data, and services to a known good state from backups or other secure sources.
- **System Validation**: Verify the integrity and functionality of restored systems and data to ensure they are fully operational and secure.

6.Lessons Learned:

- **Post-Incident Review**: Conduct a post-incident review or debriefing session to analyze the incident response process, identify strengths and weaknesses, and gather lessons learned.
- **Documentation**: Document findings, actions taken, and recommendations for improvements in incident response procedures, policies, and technical controls.
- **Continuous Improvement**: Implement recommended improvements and updates based on lessons learned to enhance the organization's overall incident response capabilities.

7.Reporting and Communication:

- **Internal Reporting**.
- **External Reporting**.

Type of Logs

1. System Logs
- **Operating System Logs**: Record events related to the operating system, such as boot events, shutdowns, crashes, and system updates.

2. Application Logs
- **Definition**: Capture events related to the functioning of applications and software.
- **Examples**: Logs from web servers (Apache, Nginx), database servers (MySQL, PostgreSQL), and custom applications.

3. Security Logs
- **Definition**: Record security-related events, such as authentication attempts, access control decisions, and policy changes.
- **Examples**: Firewall logs, Intrusion Detection/Prevention System (IDS/IPS) logs, antivirus logs.

4. Network Logs
- **Definition**: Capture data about network traffic and events related to network devices.
- **Examples**: Router and switch logs, VPN logs, network flow data (NetFlow, sFlow).

6. Web Server Logs
- **Definition**: Record HTTP requests and responses handled by web servers.
- **Examples**: Access logs, error logs, and request logs from servers like Apache, Nginx, IIS.

7. Database Logs
- **Definition**: Capture events related to database operations, queries, and transactions.
- **Examples**: SQL query logs, transaction logs, error logs from databases like MySQL, Oracle, SQL Server.

8. Email Logs
- **Definition**: Record email transactions and related activities.
- **Examples**: SMTP logs, mail server logs (Postfix, Exchange), spam filter logs.

9. Authentication Logs
- **Definition**: Capture details about authentication attempts and outcomes.
- **Examples**: Login attempts, successful and failed authentications, multi-factor authentication (MFA) events.

10. Firewall Logs
- **Definition**: Record traffic allowed or blocked based on firewall rules.
- **Examples**: Packet logs, connection attempts, rule matches.

11. IDS/IPS Logs
- **Definition**: Capture alerts and events related to intrusion detection and prevention systems.
- **Examples**: Snort logs, Suricata logs, alert logs.

12. Endpoint Logs
- **Definition**: Record events and activities on endpoint devices, such as desktops and laptops.
- **Examples**: Antivirus scans, endpoint detection and response (EDR) logs, application usage.

Protocol Logs

1. HTTP/HTTPS Logs

Access Logs

- **Timestamp**: Date and time of the request.
- **Client IP Address**: IP address of the requesting client.
- **HTTP Method**: Method used (e.g., GET, POST).
- **Request URI**: The requested resource.
- **HTTP Version**: Version of the HTTP protocol used.
- **Response Status Code**: HTTP status code returned by the server.
- **User-Agent**: Information about the client's browser or software.
- **Referer**: The URL of the previous web page from which a link to the currently requested page was followed.
- **Bytes Sent**: Amount of data sent to the client.

Error Logs

- **Timestamp**: Date and time of the error.
- **Client IP Address**: IP address of the client that caused the error.
- **Error Message**: Description of the error encountered.
- **Request URI**: The resource requested when the error occurred.

2. DNS Logs

Query Logs

- **Timestamp**: Date and time of the query.
- **Client IP Address**: IP address of the querying client.
- **Query Name**: The domain name requested.
- **Query Type**: Type of DNS query (e.g., A, AAAA, MX).
- **Response Code**: DNS response code indicating the status of the query.

Response Logs

- **Timestamp**: Date and time of the response.
- **Client IP Address**: IP address of the querying client.
- **Query Name**: The domain name requested.
- **Query Type**: Type of DNS query.
- **Response Data**: Data returned in the DNS response (e.g., IP addresses).

3. SMTP Logs

Mail Server Logs

- **Timestamp**: Date and time of the email transaction.
- **Client IP Address**: IP address of the sending or receiving client.
- **Sender Address**: Email address of the sender.
- **Recipient Address**: Email address of the recipient.
- **Message ID**: Unique identifier for the email message.
- **Status Code**: SMTP status code indicating the result of the transaction.
- **Error Message**: Description of any error encountered.

4. FTP Logs

Transfer Logs

- **Timestamp**: Date and time of the file transfer.
- **Client IP Address**: IP address of the client.
- **Username**: Username of the client.
- **Command**: FTP command executed (e.g., RETR, STOR).
- **File Path**: Path of the file transferred.
- **Transfer Size**: Size of the file transferred.
- **Status Code**: Result of the transfer (e.g., success, failure).

5. SSH Logs

Authentication Logs

- **Timestamp**: Date and time of the login attempt.
- **Client IP Address**: IP address of the connecting client.
- **Username**: Username used for the login attempt.
- **Authentication Method**: Method used (e.g., password, public key).
- **Result**: Success or failure of the login attempt.

Command Execution Logs

- **Timestamp**: Date and time of command execution.
- **Client IP Address**: IP address of the client.
- **Username**: Username of the logged-in user.
- **Command**: Command executed.

6. IMAP/POP3 Logs

Connection Logs

- **Timestamp**: Date and time of the connection.
- **Client IP Address**: IP address of the connecting client.
- **Username**: Username used for the connection.
- **Command**: Command executed (e.g., LOGIN, FETCH).
- **Result**: Success or failure of the command.

7. Kerberos Logs

Ticket Granting Logs

- **Timestamp**: Date and time of the ticket event.
- **Client IP Address**: IP address of the client.
- **Username**: Username of the client.
- **Ticket Type**: Type of ticket (TGT or service ticket).
- **Result**: Success or failure of the ticket issuance or usage.

Windows Logs

providing detailed information about system events, user activities, security incidents, and application behavior.

1. System Logs

- **Purpose**: Record events related to the operating system and its components.
- **Common Fields**:
  - **Date and Time**: When the event occurred.
  - **Event ID**: Unique identifier for the event.
  - **Source**: The component that generated the event.
  - **Level**: Severity of the event (e.g., Information, Warning, Error, Critical).
  - **User**: The user account associated with the event, if applicable.
  - **Computer**: The name of the computer where the event occurred.
  - **Description**: Detailed information about the event.

2. Application Logs

- **Purpose**: Record events related to software applications running on the system.
- **Common Fields**:
  - **Date and Time**, **Event ID**, **Source**, **Level**, **User**, **Computer**, **Description**.

3. Security Logs

- **Purpose**: Record security-related events, including successful and failed login attempts, privilege use, and changes to security settings.
- **Common Fields**:
  - **Date and Time**, **Event ID**, **Source**, **Level**, **User**, **Computer**, **Description**.
  - **Category**: The category of the event (e.g., Logon/Logoff, Object Access, Account Management).

4. Setup Logs

- **Purpose**: Record events related to the installation and setup of the system and applications.
- **Common Fields**:
  - **Date and Time**, **Event ID**, **Source**, **Level**, **User**, **Computer**, **Description**.

Common Event IDs and Their Descriptions

Security Logs

- **4624**: An account was successfully logged on.
- **4625**: An account failed to log on.
- **4648**: A logon was attempted using explicit credentials.
- **4672**: Special privileges assigned to a new logon.
- **4720**: A user account was created.
- **4723**: An attempt was made to change an account's password.
- **4740**: A user account was locked out.

System Logs

- **6005**: The event log service was started.
- **6006**: The event log service was stopped.
- **6008**: The previous system shutdown was unexpected.
- **41**: The system has rebooted without cleanly shutting down first (Kernel-Power).

Application Logs

- **1000**: Application error.
- **1001**: Windows Error Reporting.

Common Account Management Event IDs

- **4722**: A user account was enabled.
- **4723**: An attempt was made to change an account's password.
- **4724**: An attempt was made to reset an account's password.
- **4725**: A user account was disabled.
- **4726**: A user account was deleted.
- **4732**: A member was added to a security-enabled local group.
- **4733**: A member was removed from a security-enabled local group.
- **4738**: A user account was changed.
- **4740**: A user account was locked out.
- **4741**: A computer account was created.
- **4742**: A computer account was changed.
- **4743**: A computer account was deleted.
- **4756**: A member was added to a security-enabled universal group.
- **4757**: A member was removed from a security-enabled universal group.
- **4767**: A user account was unlocked.

Scheduled Tasks

- **4698**: A scheduled task was created.
- **4699**: A scheduled task was deleted.
- **4700**: A scheduled task was enabled.
- **4701**: A scheduled task was disabled.
- **4702**: A scheduled task was updated.

Audit Policy Changes

- **4719**: System audit policy was changed.
- **4902**: The per-user audit policy table was created.
- **4904**: An attempt was made to register a security event source.
- **4905**: An attempt was made to unregister a security event source.

Process Tracking Events

- **4688**: A new process has been created.
- **4689**: A process has existed.

Kerberos

Kerberos is a network authentication protocol designed to provide strong authentication for client-server applications by using secret-key cryptography.

The main components of Kerberos are:

- **Authentication Server (AS):**

The Authentication Server performs the initial authentication and ticket for Ticket Granting Service.

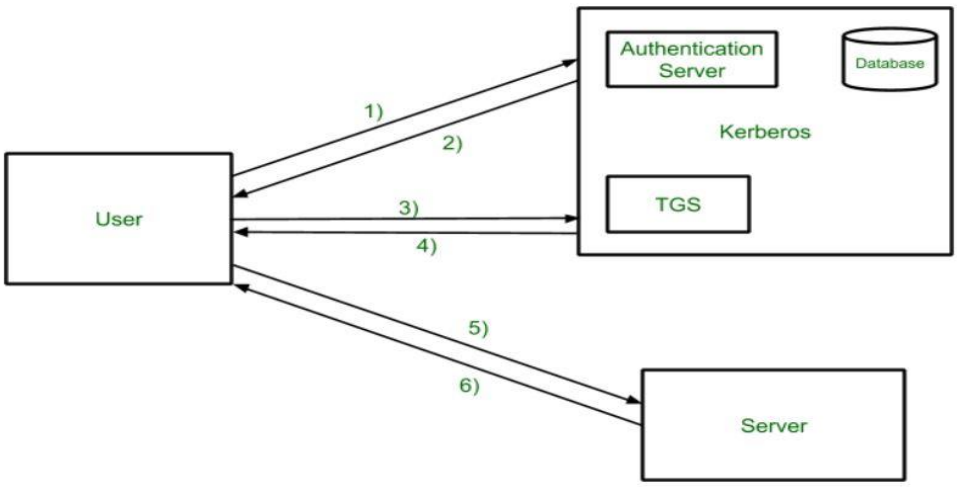
- **Database:**

The Authentication Server verifies the access rights of users in the database.

- **Ticket Granting Server (TGS):**

The Ticket Granting Server issues the ticket for the Server.

Kerberos Overview:



Step-1:

User login and request services on the host. Thus, user requests for ticket-granting service.

Step-2:

Authentication Server verifies user's access right using database and then gives ticket-granting-ticket and session key. Results are encrypted using the Password of the user.

Step-3:

The decryption of the message is done using the password then send the ticket to Ticket Granting Server. The Ticket contains authenticators like user names and network addresses.

Step-4:

Ticket Granting Server decrypts the ticket sent by User and authenticator verifies the request then creates the ticket for requesting services from the Server.

Step-5:

The user sends the Ticket and Authenticator to the Server.

Step-6:

The server verifies the Ticket and authenticators then generate access to the service. After this User can access the services.

Common Kerberos Attacks

1. **Pass-the-Ticket (PtT)**:
    - Attackers steal Kerberos tickets from a compromised system and use them to authenticate to other systems within the network. This bypasses the need for credentials like passwords.

2. **Pass-the-Hash (PtH)**:
    - Involves stealing hashed credentials (password hashes) and using them to authenticate as a user. Although this is more commonly associated with NTLM, similar principles can apply to Kerberos environments.

3. **Overpass-the-Hash (Pass-the-Key)**:
    - Attackers use NTLM hashes to request Kerberos tickets, effectively combining elements of PtH and PtT. This can grant an attacker Kerberos tickets using stolen NTLM hashes.

4. **Golden Ticket Attack**:
    - Attackers create a forged TGT with an indefinite expiration date and elevated privileges (e.g., domain administrator). This requires obtaining the Kerberos Ticket Granting Ticket (KRBTGT) account hash, which is highly privileged.

Mitigating Kerberos Attacks:

1. **Strong Password Policies**: Enforce strong, complex passwords for all accounts, especially service and privileged accounts.

2. **Regular Account Audits**: Regularly audit and review accounts for proper permissions and activity.

3. **Limit Privileges:** Follow the principle of least privilege, ensuring accounts have only the access they need.

4. **Multi-Factor Authentication (MFA)**: Implement MFA to add an additional layer of security.

5. **Monitor and Detect**: Use security monitoring tools to detect unusual behavior and potential attacks on Kerberos tickets and authentication processes.

6. **Patch and Update**: Keep systems and software up to date with the latest patches to mitigate known vulnerabilities.

SAM

The Security Accounts Manager (SAM) is a database file in Windows operating systems that stores user account information, including usernames and hashed passwords. It is used by Windows to manage local user and group accounts.

key points about SAM in Windows:

1. **Location**: located in the `C:\Windows\System32\config` directory.

2. **Function**: SAM is responsible for authenticating users when they log in to the system. It compares the entered credentials against the stored hashes in the database.

3. **Security**: Access to the SAM file is restricted to prevent unauthorized access to user account information. It is protected by the system and can only be accessed by processes with the appropriate permissions, such as the Local Security Authority Subsystem Service (LSASS).

4. **Registry**: The SAM database is also represented in the Windows registry under `HKEY_LOCAL_MACHINE\SAM`.

NTLM

NTLM (NT LAN Manager) is a suite of Microsoft security protocols intended to provide authentication, integrity, and confidentiality to users. NTLM is used for authentication purposes in various Microsoft network protocols.

key points about NTLM:

1. **Authentication Protocol**: NTLM is a challenge-response authentication protocol that uses a three-way handshake process to authenticate a client to a server. It is used to authenticate clients in a connectionless environment, as well as to provide session security in a connection-oriented environment.

2. **Use Cases**: NTLM is commonly used in situations where Kerberos (a more secure and preferred authentication protocol) cannot be used. This includes:
   - Authenticating local logins on non-domain joined systems.
   - Authenticating users in a workgroup environment.
   - Providing backward compatibility with older systems and applications.

3. **Security Concerns:** NTLM has several security weaknesses, including susceptibility to relay attacks, pass-the-hash attacks, and brute-force attacks due to the weaker hashing algorithms used in NTLMv1 and earlier versions. Consequently, it is recommended to use Kerberos wherever possible and restrict the use of NTLM.

4. **Working Mechanism:**

   - **Client sends a negotiate message** to the server to establish capabilities.
   - **Server responds with a challenge message** containing a random number (nonce).
   - **Client responds with an authenticate message** that includes the username and a hashed value, which is computed using the user's password and the nonce.

5. **Hashing and Encryption**: NTLMv2 uses stronger cryptographic algorithms (MD5 and HMAC-MD5) compared to the earlier versions, improving security.

Phishing Emails

Phishing emails are a type of cyber-attack where attackers disguise themselves as legitimate entities to trick individuals into **<u>revealing sensitive information such as usernames, passwords, credit card numbers, and other personal data.</u>**
These emails often contain malicious links or attachments that can install malware or direct the user to fraudulent websites designed to steal information.

Types of Phishing Emails

1. **Spear Phishing**:
    - **Targeted Attack**: Directed at specific individuals or organizations.
    - **Example**: An email that appears to come from a trusted colleague or superior, asking for sensitive information or prompting a malicious action.
2. **Clone Phishing**:
    - **Clone of a Legitimate Email**: Attackers create a nearly identical copy of a legitimate email that the victim has previously received, but with malicious links or attachments.
    - **Example**: An email that looks like a previously received invoice but contains a malicious link.
3. **Whaling**:
    - **High-Value Targets**: Targets high-profile individuals such as executives or high-ranking officials within an organization.
    - **Example**: An email impersonating a CEO asking for sensitive company information or authorizing a wire transfer.
4. **Vishing and Smishing**:
    - **Voice and SMS Phishing**: Variants of phishing that use voice calls (vishing) or text messages (smishing) to trick victims into revealing personal information.
    - **Example**: A text message claiming to be from a bank, asking the recipient to click a link and verify account details.

Common Tactics Used in Phishing Emails

1. **Urgency and Fear**:
    - Creating a sense of urgency or fear to prompt immediate action without thinking.
    - Example: "Your account will be locked if you don't verify your information within 24 hours."
2. **Spoofed Sender Addresses**:
    - Using email addresses that look similar to legitimate ones.
    - Example: support@paypal.com vs. support@paipal.com.
3. **Compelling Subject Lines**:
    - Using attention-grabbing subject lines to entice recipients to open the email.
    - Example: "Urgent: Invoice Overdue" or "You've won a prize!"
4. **Malicious Links and Attachments**:
    - Including links that lead to fraudulent websites or attachments that contain malware.

Defense Against Phishing Emails

1. **User Education and Training**:
   - Regularly train employees to recognize phishing attempts and understand the dangers of phishing.
   - Conduct simulated phishing attacks to test and improve employees' awareness and response.
2. **Email Filtering and Anti-Phishing Tools**:
   - Use advanced email filtering solutions that can detect and block phishing emails.
   - Implement anti-phishing software and browser extensions that warn users about suspicious websites and emails.
3. **Multi-Factor Authentication (MFA)**:
   - Require MFA for accessing sensitive systems and information. Even if credentials are compromised, attackers will have a harder time gaining access.
4. **Secure Email Gateways**:
   - Use secure email gateways to scan incoming emails for known phishing indicators, malware, and suspicious attachments.
5. **Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting, and Conformance (DMARC):**
   - Implement these email authentication protocols to prevent email spoofing and ensure that emails sent from your domain are legitimate.

SPF, DKIM, and DMARC

1. Sender Policy Framework (SPF)

Purpose: To prevent email spoofing by allowing domain owners to specify which mail servers are authorized to send email on behalf of their domain.

How It Works:

- **DNS Record**: The domain owner publishes an SPF record in the Domain Name System (DNS). This record is a list of IP addresses or hostnames authorized to send emails for the domain.
- **Email Verification**: When an email is received, the recipient's mail server checks the SPF record of the sending domain. If the sending server's IP address is listed in the SPF record, the email is considered legitimate.
- **Outcome**: Based on the SPF check, the recipient's server can accept, reject, or flag the email as suspicious.

Example: An SPF record might look like this:

v=spf1 ip4:192.168.0.1 include: spf.google.com -all

This record authorizes the IP address 192.168.0.1 and Google's mail servers to send emails on behalf of the domain.

2. DomainKeys Identified Mail (DKIM)

Purpose: To ensure the integrity and authenticity of an email by allowing the receiver to verify that the email was sent and authorized by the owner of the domain.

How It Works:

- **Digital Signature**: The sending mail server signs outgoing emails with a private key, creating a unique DKIM signature in the email header.
- **DNS Record**: The domain owner publishes the public key in a DKIM record in the DNS.
- **Email Verification**: The recipient's mail server retrieves the public key from the DNS and uses it to verify the signature. If the signature matches, it confirms that the email has not been altered and is genuinely from the claimed domain.
- **Outcome**: A valid DKIM signature ensures the email content is intact and from a legitimate sender.

Example: A DKIM signature in an email header might look like this:

```
DKIM-Signature: v=1; a=rsa-sha256; d=example.com; s=selector1; h=from:to:subject;
  bh=base64hashvalue;
  b=base64signature;
```

3. Domain-based Message Authentication, Reporting, and Conformance (DMARC)

Purpose: To provide a policy framework that uses SPF and DKIM to detect and prevent email spoofing. It also provides mechanisms for reporting authentication failures.

How It Works:

- **DNS Record**: The domain owner publishes a DMARC record in the DNS, specifying the policy for handling emails that fail SPF or DKIM checks.
- **Alignment**: DMARC requires that the domain in the "From" address aligns with the domains used in the SPF and DKIM checks.
- **Policy Enforcement**: Based on the DMARC policy, the recipient's mail server decides how to handle emails that fail authentication (e.g., reject, quarantine, or accept them).
- **Reporting**: DMARC provides reporting mechanisms where the recipient's mail server can send reports back to the domain owner about authentication failures.

Example: A DMARC record might look like this:

```
v=DMARC1; p=reject; rua=mailto:dmarc-reports@example.com; ruf=mailto:dmarc-failures@example.com; adkim=s; aspf=s
```

Combined Use of SPF, DKIM, and DMARC

Using SPF, DKIM, and DMARC together provides a robust email authentication mechanism:

1. **SPF**: Verifies that the email comes from an authorized server.
2. **DKIM**: Ensures the email content has not been tampered with and confirms the sender's identity.
3. **DMARC**: Enforces policies on how to handle emails failing SPF and DKIM checks and provides feedback to the domain owner.

Attacker techniques to evade email phishing detection?

- **1-New created domain.**
- **2-Using non-blacklisted SMTP servers.**
- **3-if the victim uses Sandbox before opening the mail so the attacker uses Sandbox evasion techniques.**

Identifying Phishing Emails

1. **Check the Sender's Email Address**:
   - Look for subtle misspellings or unusual domain names.
2. **Hover Over Links**:
   - Hover over links without clicking to see the actual URL. Verify that it points to a legitimate site.
3. **Look for Poor Grammar and Spelling**:
   - Many phishing emails contain noticeable grammatical errors and spelling mistakes.
4. **Be Wary of Urgency and Unusual Requests**:
   - Be skeptical of emails that create a sense of urgency or request sensitive information.
5. **Verify with the Source**:
   - If in doubt, contact the supposed sender directly using a known, legitimate communication channel to verify the email's authenticity.

What would we collect during the email investigation?

- Sender email address
- Sender IP address
- Email subject line
- Recipient email address
- Reply-to email address (if any)
- Date/time
- Any URL links (if an URL shortener service was used, then we'll
- need to obtain the real URL link)
- The name of the attachment
- The hash value of the attachment (hash type MD5 or SHA256)

Email Flow

1. Composition→Sender's Email Client (MUA - Mail User Agent):

- **Action**: composes an email using an email client (e.g., Outlook, Gmail, Thunderbird).
- **Components**: The email includes the sender's address, recipient's address, subject, body, and any attachments.

2. Submission→Mail Submission Agent (MSA):

- **Action**: the email client forwards the email to the MSA.
- **Port**: Typically uses port 587 or 465 for secure submission.

3. Processing→Mail Transfer Agent (MTA):

- **Action**: The MSA hands the email over to the MTA, which is responsible for routing the email to its destination.
- **DNS Lookup**: The MTA performs a DNS lookup to find the recipient's mail server by querying the MX (Mail Exchange) records of the recipient's domain.

4. Delivery→Recipient's Mail Server (MX Server):

- **Action**: The final MTA delivers the email to the recipient's mail server, identified by the MX records.
- **Security Checks**: The recipient's mail server may perform various security checks, including **SPF, DKIM, and DMARC** validations, spam filtering, and malware scanning.

5. Receipt→Mail Delivery Agent (MDA):

- **Action**: MDA receives the email from the recipient's mail server and stores it in the recipient's mailbox until accessed by the user.

6. Access→Recipient's Email Client (MUA):

- **Protocols**: The email client uses protocols like **IMAP** (Internet Message Access Protocol) or **POP3** (Post Office Protocol) to retrieve emails from the mail server.
    - **IMAP (Port 143/993):** Allows the email client to access and manipulate the email stored on the mail server **without downloading them.**
    - **POP3 (Port 110/995)**: Downloads the email from the mail server to the client and **usually deletes it from the server.**

Activities That Indicate Malicious Behavior

1. Network Activity

1. **Unusual Traffic Patterns**:
    - **Large data transfers to external IP addresses.**
    - Unusual port activity, especially on non-standard ports.

2. **Connections to Known Malicious IPs**:
    - Communication with IP addresses known to be associated with malware, botnets, or cybercriminal activity.

3. **Lateral Movement**:
    - **Internal network scanning.**
    - Unusual access attempts from one internal system to another.
    - Use of administrative tools like PsExec, PowerShell, or WMI to move laterally within the network.

2. User Behavior

1. **Unusual Login Patterns**:
    - **Multiple failed login attempts.**
    - **Logins from unfamiliar locations or IP addresses.**

2. **Access Anomalies**:
    - **Access to sensitive data or systems not typically used by the user.**
    - Multiple logins from different locations within a short period.

3. Endpoint Activity

1. **Process Anomalies**:
    - Execution of uncommon processes or applications.
    - **Unexpected or unauthorized use of system utilities (e.g., PowerShell, Command Prompt).**

2. **File Activity**:
    - **Creation or modification of system files.**
    - Presence of new or unknown files in system directories.
    - Large numbers of files being encrypted (indicative of ransomware).

3. **Registry Changes**:
    - **Unauthorized changes to the Windows registry**, often used to maintain persistence.

4. Application Activity

1. **Anomalous Application Behavior**:
    - Applications crashing frequently or behaving unexpectedly.
    - Applications attempting to connect to external systems without justification.

2. **Suspicious Scripts or Macros**:
    - Execution of scripts or macros in documents, especially from email attachments.
    - PowerShell scripts running without obvious cause.

5. Email Activity

1. **Phishing Indicators**:
    - Links or attachments from unknown or suspicious senders.
    - Spoofed email addresses resembling legitimate ones.

2. **Unusual Sending Patterns**:
    - **High volume of outbound emails in a short time frame.**
    - Emails being sent to unusual or unexpected recipients.

6. System and Application Logs

1. **Log Anomalies**:
    - Unexplained gaps or deletions in logs.

2. **Privilege Escalation Attempts**:
    - **Attempts to modify system configurations or security settings.**
    - Unauthorized access to administrative accounts or security tools.

7. External Indicators

1. **Threat Intelligence Feeds**:
    - Alerts from threat intelligence sources about new vulnerabilities, threats, or active attacks targeting the organization.
2. **Compromised Accounts**:
    - Reports of compromised accounts or credentials on the dark web.

Defensive Measures and Detection Strategies

1. **Network Monitoring**:
    - Implement network intrusion detection and prevention systems (IDS/IPS).
    - Use security information and event management (SIEM) systems to aggregate and analyze log data.
2. **User and Entity Behavior Analytics (UEBA)**:
    - Utilize UEBA tools to detect anomalies in user behavior patterns.
    - Set up alerts for unusual login attempts, privilege escalation, and data access.
3. **Endpoint Detection and Response (EDR)**:
    - Deploy EDR solutions to monitor and respond to suspicious endpoint activities.
    - Regularly update antivirus and anti-malware tools.
4. **Access Controls and Policies**:
    - Enforce the principle of least privilege (PoLP) for user accounts and access controls.
    - Implement multi-factor authentication (MFA) to secure access to critical systems.
5. **Email Security**:
    - Use email filtering solutions to block phishing and malicious emails.
    - Educate users on recognizing phishing attempts and suspicious emails.
6. **Regular Audits and Penetration Testing**:
    - Conduct regular security audits and vulnerability assessments.
    - Perform penetration testing to identify and mitigate potential weaknesses.

NetBIOS

NetBIOS (Network Basic Input/Output System):

- **Definition**: NetBIOS is a networking protocol used for communication between devices on a local area network (LAN).
- **Functions**: It provides services related to the session layer of the OSI model, including name resolution (NetBIOS Name Service - NBNS), session establishment, and data transfer.
- **Legacy Protocol**: Originally developed by IBM, NetBIOS became a standard for LAN communication, especially in Microsoft Windows environments.
- **Usage**: While largely replaced by more modern protocols like TCP/IP, NetBIOS is still used in some legacy systems and applications.
- **Ports**:
    - **137 (NetBIOS Name Service).**
    - **138 (NetBIOS Datagram Service).**

- **139 (NetBIOS Session Service) for communication.**

SMB

- **Definition**: SMB is a network file sharing protocol that allows applications on a computer to read and write to files and request services from server programs in a computer network.
- **Functions**: It operates at the application layer of the OSI model and facilitates shared access to files, printers, serial ports, and miscellaneous communications between nodes on a network.
- **Versions**: Over time, SMB has evolved through different versions (SMB1, SMB2, SMB3), each offering improved performance, security features, and capabilities.
- **Security Concerns**: Older versions of SMB, especially SMB1, have known security vulnerabilities (like the WannaCry ransomware exploit), prompting organizations to disable or upgrade to newer versions.

Digital Certificates

- **Definition**: A digital certificate is an electronic document used to prove the ownership of a public key. It includes information about the key, the owner's identity, and the digital signature of an entity that has verified the certificate's contents.
- **Issuance**: Certificates are typically issued by a certificate authority (CA), a trusted third party that verifies the identity of the certificate holder.

- **Components**:
  - Public Key of the Certificate Holder
  - Identity of the Certificate Holder (e.g., name, email address)
  - Issuer (CA) Information
  - Digital Signature of the Issuer
  - Validity Period (start and end dates)

- **Usage**: Digital certificates are used in various security protocols and applications, including:
  - **SSL/TLS**: Securing websites and encrypting data transmitted over the internet.
  - **Code Signing**: Authenticating the source of software and ensuring it has not been tampered with.
  - **Email Security**: Encrypting and digitally signing emails to verify sender identity and protect message integrity.

- **Authentication**: Providing secure access to networks and systems (e.g., VPNs, Wi-Fi networks).

SIEM Solutions

SIEM stands for Security Information and Event Management.
A centralized node analyzes current or historical events and logs data, perform event correlation and threat monitoring → **(Event Management).**
Index and parsing logs data from disparate device or sources for analysis and reports→ (**Information Management**).

Key Components and Functions of SIEM Solutions:

1. **Data Collection**:
   - **Log Management**: Collects and stores logs and events from a wide range of sources such as network devices, servers, applications, databases, and endpoints.
   - **Event Correlation**: Aggregates and correlates security events to identify patterns and potential threats.
2. **Normalization and Parsing**:
   - Converts raw event data from different sources into a standardized format for easier analysis and correlation.
3. **Alerting and Monitoring**:
   - **Real-time Monitoring**: Monitors incoming events in real-time to detect security incidents as they occur.
   - **Alerting**: Generates alerts and notifications for suspicious activities or potential security breaches based on predefined rules and thresholds.
4. **Incident Detection and Response**:
   - **Threat Detection**: Uses advanced analytics, machine learning, and threat intelligence to identify known and unknown threats.
   - **Incident Response**: Provides workflows and tools for investigating and responding to security incidents promptly.
5. **Forensic Analysis and Investigation**:
   - Enables security teams to conduct detailed forensic analysis of security events and incidents.
6. **Compliance Reporting**:

- Helps organizations comply with regulatory requirements by generating audit reports and providing evidence of security controls and activities.

7. **User and Entity Behavior Analytics (UEBA)**:
    - Analyzes user behavior and entity activities to detect anomalies and insider threats.
    - Helps in identifying compromised accounts or malicious insider activities.

Benefits of SIEM Solutions:

- **Centralized Visibility**: Provides a centralized view of the organization's security posture and events across the entire IT infrastructure.
- **Early Threat Detection**: Helps in early detection of security incidents and threats before they cause significant damage.
- **Response Efficiency**: Improves incident response times by automating alerting, investigation, and remediation processes.
- **Compliance Support**: Facilitates compliance with regulatory requirements through continuous monitoring and reporting.
- **Operational Efficiency**: Streamlines security operations by reducing manual efforts and improving efficiency through automation.

Challenges:

- **Complexity**: Implementing and managing SIEM solutions can be complex and resource-intensive.
- **Tuning and False Positives**: Requires tuning to reduce false positives and ensure accurate threat detection.
- **Skill Requirements**: Requires skilled security personnel to configure, operate, and interpret SIEM data effectively.

Conclusion:

SIEM solutions play a critical role in modern cybersecurity strategies by providing proactive threat detection, incident response capabilities, and compliance support. They enable organizations to monitor, analyze, and respond to security events in real-time, thereby enhancing overall security posture and resilience against cyber threats.

Definitions

1.Confidentiality: Ensuring that only authorized individuals have access to sensitive information. This can be achieved through encryption, access controls, and data classification.
2. **Integrity:** Maintaining the accuracy and trustworthiness of data. Measures like data validation, checksums, and version controls help prevent unauthorized modifications.
3. **Availability:** Ensuring that information and resources are accessible when needed. Redundancy, backup systems, and disaster recovery plans contribute to maintaining availability.
4. **Authentication:** Verifying the identity of users and systems. This is done through passwords, biometrics, and multi-factor authentication.
5. **Authorization:** Granting appropriate levels of access to authorized users. Access control lists, role-based access control (RBAC), and least privilege principles are used to enforce authorization.
6. **Risk Management:** Identifying potential risks and vulnerabilities, assessing their potential impact, and implementing measures to mitigate or manage those risks.
7. **Security Awareness and Training:** Educating employees and users about security best practices and potential threats to increase awareness and promote responsible behavior.
8. **Vulnerability Management:** Regularly scanning and assessing systems for vulnerabilities and applying patches or updates to mitigate potential exploits.
9. **Intrusion Detection and Prevention:** Deploying tools and systems to detect and prevent unauthorized access or malicious activities within a network or system.
10. **Security Policies and Procedures:** Establishing clear security policies, guidelines, and procedures that govern how information should be handled, shared, and protected.
11. **Incident Response:** Developing a plan to respond to security incidents, including containment, investigation, and recovery.
12. **Physical Security:** Protecting physical assets such as servers, data centers, and networking equipment from unauthorized access.
13. **Cryptography:** Using encryption techniques to secure data both in transit and at rest.
14.Network Security: Implementing firewalls, intrusion detection systems, and other measures to protect networks from external threats.
15.Application Security: Ensuring that software applications are developed, tested, and maintained with security in mind to prevent vulnerabilities.
15.Trust but Verify: we should always verify even when we trust an entity and its behavior. An entity might be a user or a system.
16.Zero Trust: "never trust, always verify."

example of common security vulnerabilities?

1. **Unpatched Software:** Failing to regularly update and patch software can leave vulnerabilities open that attacker can exploit. Hackers often target known vulnerabilities for which patches have been released.
2. **Weak Passwords:** Using easily guessable passwords or default can allow attackers to gain unauthorized access to systems and accounts.
3. **Lack of Encryption:** Failing to encrypt sensitive data.
4. **SQL Injection:** Improperly validated input in web applications can allow attackers to inject malicious SQL code, potentially granting them unauthorized access to databases.
5. **Cross-Site Scripting (XSS):** Insufficient input validation in web applications can enable attackers to inject malicious scripts into web pages viewed by other users, potentially stealing their information or compromising their sessions.
6. **Phishing:** Employees falling victim to phishing emails can lead to credential theft or malware infection.
7. **Insider Threats:** Employees or contractors with malicious intent or inadequate security training can misuse their access privileges.
8. **Social Engineering:** Attackers can manipulate individuals into disclosing confidential info or performing actions that compromise security.
9. **Remote Work Risks:** Inadequately secured remote work environments can lead to unauthorized access, data leakage, and other security breaches.

INCIDENT RESPONSE FOR COMMON ATTACK TYPES

1. Brute Forcing

Details:

Attacker trying to guess a password by attempting several different passwords

Threat Indicators:

Multiple login failures in a short period of time

Where To Investigate:

- Active directory logs, Application logs, Operational system logs, Contact user

Possible Actions:

If not legit action, disable the account and investigate/block attacker

2. Botnets

Details:

Attackers are using the victim server to perform DDoS attacks or other malicious activities

Threat Indicators:

- Connection to suspicious IPs
- Abnormal high volume of network traffic

Where To Investigate:

- Network traffic, OS logs (new processes), Contact server owner, Contact support team

Possible Actions:

If confirmed:

- Isolate the server
- Remove malicious processes
- Patch the vulnerability utilized for infection

3. Ransomware

Details:

A type of malware that encrypts files and requests a ransom (money payment) from the user to decrypt the files

Threat Indicators:

- Anti-Virus alerts
- Connection to suspicious Ips

Where To Investigate:

- AV logs, OS logs, Account logs, Network traffic

Possible Actions:

- Request AV checks
- Isolate the machine

4. Data Exfiltration

Details:

Attacker (or rogue employee) exfiltrate data to external sources

Threat Indicators:

- Abnormal high network traffic
- Connection to cloud -storage solutions (Dropbox, Google Cloud)

Where To Investigate:

- Network traffic, Proxy logs, OS logs

Possible Actions:

- If employee: Contact manager, perform full forensics
- If external threat: Isolate the machine, disconnect from network

5. Advanced Persistent Treats (APTs)

Details:

Attackers get access to the system and create backdoors for further exploitation. Usually hard to detect

Threat Indicators:

- Connection to suspicious IPs or Abnormal high volume of network traffic or Off-hour's access logs or new admin account creations

Where To Investigate:

- Network traffic, Access logs, OS logs (new processes, new connections, abnormal users), Contact server owner/support teams

Possible Actions: Isolate the machine and start formal forensics process

OSI Layer Attacks

(1) Physical Layer

(2) Data Link Layer

- ARP Spoofing/Poisoning
- MAC Flooding

(3) Network Layer

- IP Spoofing
- IPv6 Tunneling
- Smurf Attack
- ICMP Flooding
- DHCP Spoofing
- DHCP Starvation

(4) Transport Layer

- TCP SYN Flood
- TCP Session Hijacking
- TCP Reset attack
- UDP Flooding

(5) Session Layer

- Session Hijacking

(6) Presentation Layer

- SSL → SL Striping

(7) Application Layer

- DNS
  - Zone transfer
  - DNS Spoofing
- HTTP/HTTPS
  - Web Attacks
- FTP (Plain-text protocol)
  - Brute force
  - Download critical files
  - Upload malicious files
- TELNET
  - Brute force

Identity and Access Management (IAM): - IAM it is a framework ensure that only authorized users have access to specific resources and data and that their access is monitored and controlled. IAM systems use various technologies to manage access, including role-based access control, multi-factor authentication, and single sign-on. IAM systems help organizations comply with regulatory requirements as HIPAA, GDPR

Detection categories

1. A true **positive** **is an alert that correctly detects the presence of an attack.**

2. A true **negative** **when no malicious activity exists, and no alert triggered.**

3. A false positive **is an alert that incorrectly detects the presence of a threat. This is when an IDS identifies an activity as malicious, but it isn't. False positives are an inconvenience for security teams because they spend**
time and resources investigating an illegitimate alert.

4. A false negative **is a state where the presence of a threat is not detected. This is when malicious activity happens but an IDS fails to detect it. False negatives are dangerous because security teams are left unaware of legitimate attacks that they can be vulnerable to.**

Positive	**There is Alert**
Negative	**There is no Alert**

Attack surface **is all potential Vulnerabilities that a threat actor could exploit.**

How HTTPS Work

HTTPS (Hypertext Transfer Protocol Secure) is a protocol for secure communication over a computer network, widely used on the Internet. Here's how HTTPS works in a simplified manner:

1. **Encryption**: HTTPS uses encryption to secure the data transmitted between a client (e.g., a web browser) and a server (e.g., a website).
2. **SSL/TLS Protocol**: HTTPS relies on SSL (Secure Sockets Layer) or more commonly now TLS (Transport Layer Security) protocols to establish an encrypted connection.

3. **Handshake Process**:
    - **Client Hello**: The process begins when a client (e.g., a web browser) sends a "Client Hello" message to the server, indicating its intention to establish a secure connection and presenting its supported SSL/TLS versions, encryption algorithms, and other parameters.
    - **Server Hello**: The server responds with a "Server Hello" message, selecting the best SSL/TLS version and encryption algorithm from the client's list and sending its digital certificate.
    - **Certificate Authentication**: The client verifies the server's digital certificate to ensure it is legitimate and issued by a trusted Certificate Authority (CA). This certificate contains the server's public key.
    - **Key Exchange**: Using asymmetric encryption (public-key encryption), the client and server exchange cryptographic keys to establish a secure session key for symmetric encryption (shared secret key).

4. **Secure Data Transfer**:
    - Once the secure connection is established, all data transmitted between the client and server is encrypted using the symmetric session key.
    - This encryption ensures that even if intercepted by an unauthorized party, the data cannot be easily deciphered.

5. **Authentication and Integrity**:
    - HTTPS also provides authentication and data integrity. The server's digital certificate ensures the client is connecting to the intended server and not an impostor (man-in-the-middle attack).
    - Message integrity is maintained through cryptographic hash functions, ensuring data is not altered or tampered with during transmission.
6. **Performance Considerations**:
    - While HTTPS adds overhead due to encryption and decryption processes, modern hardware and optimized protocols (like TLS 1.3) minimize performance impacts, making HTTPS widely adopted across the web.

7. **End-to-End Security**:
    - HTTPS secures not only web pages but also other data exchanged over HTTP, such as API requests, form submissions, and file downloads.

EDR (Endpoint Detection and Response)

Focus: EDR primarily focuses on monitoring and responding to security threats at the endpoint level, such as individual devices (computers, servers, mobile devices).

Capabilities:

- **Endpoint Visibility**: Provides deep visibility into endpoint activities, including process executions, file accesses, network connections, and registry changes.
- **Threat Detection**: Uses behavioral analytics, machine learning, and signature-based detection to identify suspicious activities and potential threats on endpoints.
- **Incident Response**: Facilitates rapid investigation and response to security incidents on endpoints, allowing security teams to contain and mitigate threats.
- **Forensic Analysis**: Collects and analyzes endpoint data to reconstruct the timeline of events during a security incident.
- **Endpoint Isolation**: Capable of isolating compromised endpoints from the network to prevent further spread of threats.

Benefits:

- Enhances visibility and control over endpoints, especially in distributed and remote work environments and enables quick detection and response to endpoint-based threats, reducing dwell time (the duration attackers remain undetected).

XDR (Extended Detection and Response)

Scope: XDR expands beyond endpoints to integrate and correlate data from multiple security layers, including endpoints, networks, email, and cloud environments.

Integration:

- **Data Sources**: Collects and analyzes telemetry data from various security products and sensors, such as EDR, NDR, email security, and cloud security platforms.
- **Cross-Layer Detection**: Correlates and analyzes data across these different security layers to provide a more comprehensive view of threats and attacks.

Capabilities:

- **Unified Visibility**: Offers a unified view of security events and incidents across different environments and security products.
- **Automated Response**: Uses automation and orchestration to respond to incidents across multiple layers, not just endpoints.
- **Advanced Analytics**: Utilizes advanced analytics, threat intelligence, and machine learning to detect complex and multi-stage attacks that span across different attack vectors.

Benefits:

- Provides enhanced threat detection and response capabilities by integrating and correlating data from diverse security sources and improves overall security posture by enabling faster and more accurate detection of sophisticated threats.

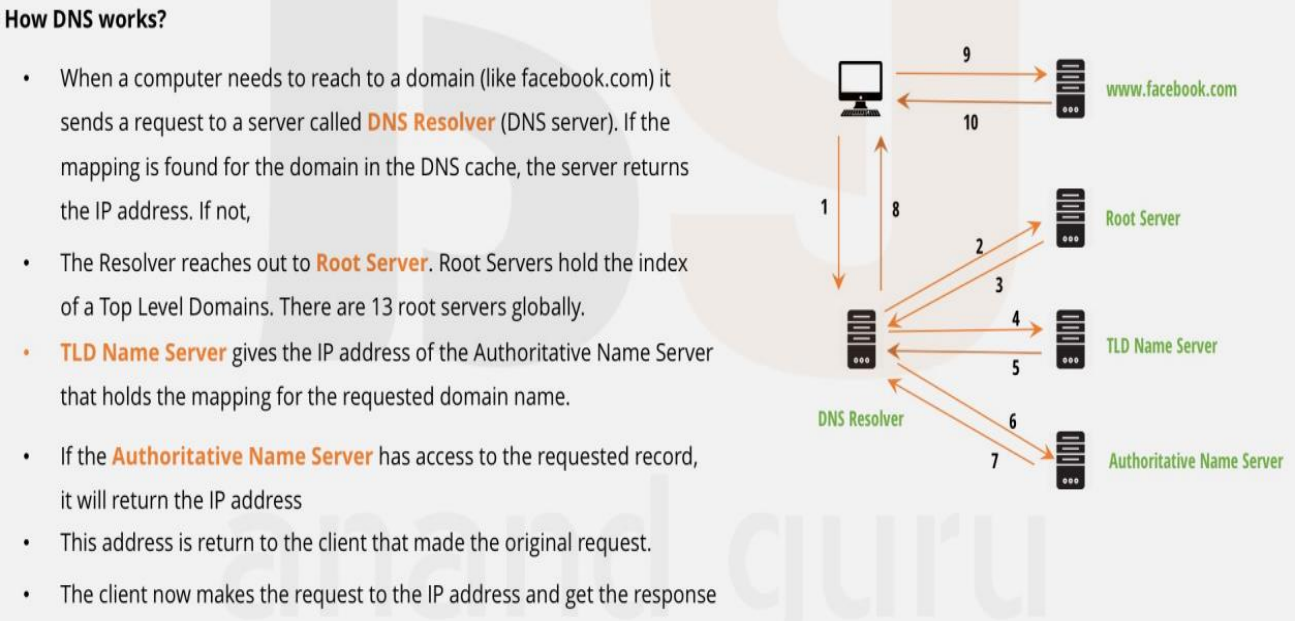
Summary:

- **EDR** focuses on endpoint-specific threat detection and response, providing deep visibility and rapid incident response capabilities at the endpoint level.

- **XDR** extends beyond endpoints to integrate and correlate telemetry data from multiple security layers, offering a unified approach to detecting and responding to threats across various attack vectors and environments.

Event is a log of a specific action such as a user login, or a VPN connection, occurs at a specific time and the event is logged at that time.

Flow is a record of network activity that can last for seconds, minutes, hours, or days, depending on the activity within the session. For example, a web request might download multiple files such as images, video, and last for 5 to 10 seconds. The flow is a record of network activity between two hosts.



MITRE ATT&CK Framework: Adversarial Tactics, Techniques, and Common Knowledge framework. It is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations.

ATT&CK helps cybersecurity professionals understand the tactics and techniques adversaries use during cyberattacks, enabling better threat detection, prevention, and response.

What is IDS?

An Intrusion Detection System (IDS) is hardware or software used to detect security breaches and attacks by monitoring a network or host.

What is IPS?

An Intrusion Prevention System (IPS) is hardware or software that detects security violations by monitoring a network or host and prevents security violations by taking the necessary action.

A firewall is a security software or hardware that monitors incoming and outgoing network traffic according to the rules it contains and allows or prevents the passage of network packets according to the nature of the rule

Some types of Firewalls:

1. Packet-Filtering Firewalls

- **Function**: Examines each packet passing through the network and accepts or rejects it based on user-defined rules.
- **Pros**: Simple and efficient for basic filtering.
- **Cons**: Limited capability in detecting complex attacks and can be bypassed.

2. Stateful Inspection Firewalls

- **Function**: Monitors the state of active connections and makes decisions based on the context of the traffic (state and packet attributes).
- **Pros**: More secure than packet-filtering as they understand the state of connections.
- **Cons**: More complex and resource-intensive.

3. Proxy Firewalls (Application-Level Gateways)

- **Function**: Acts as an intermediary between end users and the services they access, examining the traffic at the application layer.
- **Pros**: Provides deep inspection of traffic and can filter specific content.
- **Cons**: Can introduce latency and is resource-intensive.

4. Next-Generation Firewalls (NGFW)

- **Function**: Combines traditional firewall features with additional security functions like intrusion prevention, deep packet inspection, and application awareness.
- **Pros**: Offers comprehensive protection against a wide range of threats.
- **Cons**: More expensive and complex to configure and maintain.

5. Unified Threat Management (UTM) Firewalls

- **Function**: Integrates multiple security features such as firewall, VPN, antivirus, intrusion detection/prevention, and content filtering into a single device.
- **Pros**: Simplifies management and provides comprehensive security in one package.
- **Cons**: Can be a single point of failure and might not be as effective as dedicated solutions for each security function.

6. Web Application Firewalls (WAF)

- **Function**: Specifically designed to protect web applications by monitoring and filtering HTTP/HTTPS traffic.
- **Pros**: Effective against web-based attacks like SQL injection, XSS, and others.
- **Cons**: Limited to web application traffic and not suitable for protecting other types of network traffic.

7. Software Firewalls

- **Function**: Installed on individual computers or servers to protect them from unauthorized access and threats.
- **Pros**: Flexible and easy to update, suitable for individual device protection.
- **Cons**: Can consume system resources.

What log resources does Firewalls have?

Firewall products have logs about network flow because they do network-based filtering. For example:

Date/Time information, Source, Destination IP Address, Source, Destination Port, Action Information, Number of Packets Sent, and Received.

What is a Web Application Firewall (WAF)?

Is security software or hardware that **monitors, filters, and blocks incoming packets to a web application** and outgoing packets from a web application

How does a web application firewall (WAF) work?

A WAF manages inbound application traffic according to existing rules on it. These requests, which belong to the HTTP protocol, are either allowed or blocked per the rules. **Since it works at the application layer level, it can prevent web-based attacks.**

خلاص كده تقريبا خلصنا معظم الحاجات المهمة الي المفروض تراجعها والي هتفيدك بشكل كبير في أي انترفيو واي سيناريو تتعرض ليه ....

هنتكلم في كام سيناريو بقي بالإجابات بتعتهم ويبقي كده خلصنا كل حاجة.

1. **If your device gets infected with ransomware, you need to take immediate action to detect the infection and mitigate its effects. Here are the steps you should follow:**

Detecting Ransomware Infection

1. **Notice Early Signs**:
   - A **ransom message** appearing on your screen.
   - **Files become inaccessible** and have unusual extensions.
   - The device's **performance slows down** significantly.
2. **Isolate the Device**:
   - **Disconnect the infected device from the local network** and the internet immediately to prevent the ransomware from spreading to other devices.
3. **Use Security Software**:
   - **Run an antivirus or anti-malware program** to scan the entire device. Some antivirus programs may detect and remove certain types of ransomwares.
4. **Check Logs and Suspicious Activities**:
   - Examine system logs and recent activities for any signs indicating an attack or infection.

Mitigating Ransomware Infection

1. **Isolate Suspicious Files**:
   - Isolate any suspicious or infected files to prevent the ransomware from spreading.
2. **Restore from Backup**:
   - Restore your files from backups that were taken before the infection. Ensure that the backups are not stored on the same network as the infected device.
3. **Clean the Device**:
   - Use a ransomware removal tool or an antivirus program to clean the device from the ransomware.

What are the log sources?

Firewall Logs, Network logs, and Antivirus/Anti-malware Logs.

2.Phishing Attack:

Scenario:

- An employee receives a deceptive email that appears to be from a legitimate source, prompting them to click a link or download an attachment.

Response:

1. **Identify the Phishing Email:**
   - Train employees to recognize phishing emails by checking for suspicious sender addresses, generic greetings, and urgent language.
     يعنى هتقول الى اتشرح فى الميل فوق ...انك هتشوف هل الميل ده فعلا بيمثل خطر ولا لأ
2. **Contain and Report**:
   - Report the phishing email to the IT department and delete it.
   - Block the sender's email address and domain.
3. **Scan for Malware**:
   - If an attachment was downloaded, run a malware scan on the device immediately.
4. **Educate**:
   - Conduct regular training sessions on identifying and handling phishing attempts.

Logs to Check:

- **Email Server Logs:** Look for unusual email traffic or unauthorized access attempts.
- **Firewall Logs**: Check for suspicious outbound traffic or connections to known malicious IP addresses.
- **Endpoint Security Logs**: Review antivirus/anti-malware logs for detected threats.

3.Data Breach

Scenario:

- Sensitive information is accessed or stolen by an unauthorized party.

Response:

1. **Contain the Breach**:
   - Disconnect affected systems from the network to prevent further data loss.
2. **Identify and Close Vulnerabilities**:
   - Conduct a thorough investigation to identify how the breach occurred.
   - Patch any vulnerabilities and implement additional security measures.
3. **Notify Affected Parties**:
   - Notify any individuals or organizations affected by the breach.
4. **Improve Security**:
   - Conduct a comprehensive security review and enhance measures to prevent future breaches.

Logs to Check:

- **Access Logs**: Review logs from servers, databases, and applications for unauthorized access attempts.
- **System Event Logs**: Check for any unusual activity, such as failed login attempts or changes to user permissions.
- **Network Logs**: Analyze logs from firewalls and intrusion detection/prevention systems for suspicious traffic patterns.

بص يا صديقي السيناريوهات كتير اوي ومش هنخلص لكن الطريقة واحدة....

1. How to Detect

2.What will do to response

3.What is Mitigation

أتمنى أكون قدرت أحط كل حاجة مفيدة

متنساش أخوك أحمد سليمان في دعائك ومتنساش اخواتنا في فلسطين في دعائك

ولو محتاج حاجة كلمني علي لينكد ان او علي واتساب.

Mob:01097727754, User LinkedIn: ahmedsoliman19